CLAIMS

What is claimed is:

1. A network system, comprising:

a network infrastructure providing a virtual private network (VPN) and a best effort public network;

a first egress boundary router of said VPN and a second egress boundary router of said best effort public network that are each coupled for communication with an egress access network having an access link to which a destination host belonging to the VPN is coupled;

a first ingress boundary router of the VPN and a second ingress boundary router of the best effort public network, wherein said first ingress boundary router transmits only packets originating from sources within the VPN and targeting the destination host to said first egress boundary router via said VPN, and wherein said second ingress boundary router transmits packets originating from sources outside the VPN and targeting the destination host to said second egress boundary router via said best effort public network;

wherein at least said first egress boundary router is configured to transmit packets received via said VPN and targeting said destination host onto the egress access network utilizing a separate logical connection than that employed for packets communicated over the best effort public network, such that the access link is protected from denial of service attacks originating from sources outside the VPN.

2. The network system of Claim 1, wherein at least said VPN is implemented within a Differentiated Services domain.

3. The network system of Claim 1, and further comprising:

the egress access network connected to at least said first egress boundary router; and

an ingress access network connected to at least the first ingress boundary router.

4. The network system of Claim 3, wherein:

said ingress access network is connected to each of said first ingress boundary router and said second ingress boundary router;

said ingress access network has separate logical connections to said first and second ingress boundary routers for a customer premises equipment (CPE) edge router; and

said ingress access network transmits packets having both source and destination addresses belonging to the VPN to said first ingress boundary router and transmits other packets to said second ingress boundary router.

5. The network system of Claim 4, and further comprising a CPE edge router coupled to said ingress access network, wherein said CPE edge router includes a classifier that classifies at least some packets for routing to one of said first and second ingress boundary routers based at least in part on a host service markings in packet headers.

6. The network system of Claim 3, wherein:

said egress access network is connected to each of said first egress boundary router and said second egress boundary router;

said egress access network has separate logical connections to said first and second egress boundary routers for a customer premises equipment (CPE) edge router; and

said first egress boundary router transmits packets from the VPN to said CPE edge router via a first of said logical connections and said second egress boundary router transmits packets from the best effort public network to said second ingress boundary router via a second of said logical connections.

7. The network system of Claim 6, wherein said egress access network assigns a higher priority to traffic received from said first egress boundary router than traffic received from said second egress boundary router.

8. The network system of Claim 7, wherein said first egress boundary router shapes traffic destined for the destination host to prevent starvation of traffic of said second egress boundary router that is destined for the destination host.

9. The network system of Claim 6, wherein said first egress boundary router shapes traffic destined for the destination host to a first rate and said second egress boundary router

shapes traffic destined the destination host to a second rate, wherein the sum of the first and second rates is no greater than a transmission capacity of said access link.

10. The network system of Claim 1, wherein said first ingress router includes:

first and second logical input interfaces for receiving traffic destined for the VPN and for the best effort public network, respectively;

first and second logical output interfaces for transmitting traffic over the VPN and the best effort public network, respectively; and

a forwarding function that switches packets received at said first logical input interface to said first logical output interface and that switches packets received at said second logical input interface to said second logical output interface.

11. The network system of Claim 10, wherein said first egress router includes:

first and second logical input interfaces for receiving traffic from the VPN and from the best effort public network, respectively;

a first logical output interface and a second logical output interface respectively coupled to separate first and second logical connections on said egress access network, wherein said first logical output interface transmits traffic received from the VPN utilizing said first logical connection and said second logical output interface transmits traffic received from the best effort public network utilizing the second logical connection; and

a forwarding function that switches packets received at said first logical input interface to said first logical output interface and that switches packets received at said second logical input interface to said second logical output interface.

12. The network system of Claim 11, wherein said first egress boundary router includes a scheduler, coupled to each of said first and second logical output interfaces, that transmits packets from said first and second logical output interfaces onto said egress access network, wherein said scheduler grants a higher priority to traffic from said first logical output interface than to traffic from said second logical output interface.

13. The network system of Claim 12, wherein said scheduler performs work-conserving scheduling on outgoing traffic from said first and second logical output interfaces.

14. The network system of Claim 11, wherein the VPN is one of a plurality of VPNs, and wherein said forwarding function has a corresponding plurality of VPN forwarding tables and a shared forwarding table for best effort traffic.